

Gaining Total Visibility of Your Environment

Michael Smith
Information Security Engineer
TravelClick, an Amadeus company

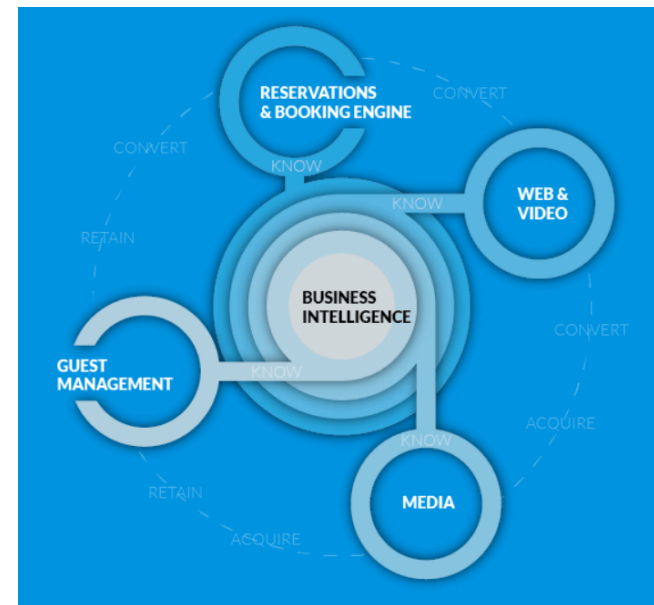
Michael Smith
Information Security Engineer
TravelClick, an Amadeus
Company

- Longtime Qualys user
- Brought Qualys into TravelClick in August



TravelClick Overview

- Provides Central Reservation Systems and Guest Management Solutions
- 25,000 independent and mid-sized hotels in 176 countries
- 1,200 employees
- 3,000 servers @ 2 datacenters (on-premise)
- Acquired by Amadeus in October 2018 for \$1.52B



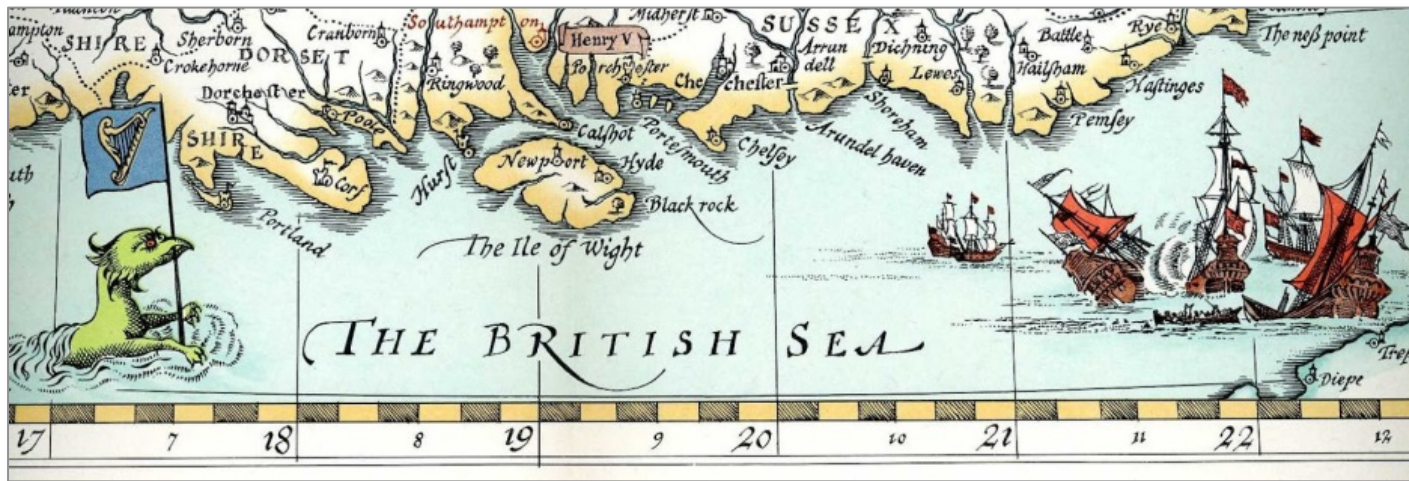
Where we came from

- Grown by acquisition – before we ourselves were acquired
- 4 acquisitions over 12 years
 - One acquisition added 40% in headcount overnight
- Everything that can be different, was different
- Managing risk by conjecture and passed-on knowledge instead of documentation and fact
- No single source of truth

Starting Point: Global IT Asset Inventory

- Biggest problem faced by every organization
- What is where?
- Who owns it? (*“Ghost Networks”*)
 - POCs stood up then ended... but still running
 - Temp projects are never temporary
 - Test environments still remaining and never decommissioned
- Who’s taking care of it?
- What’s wrong with it?

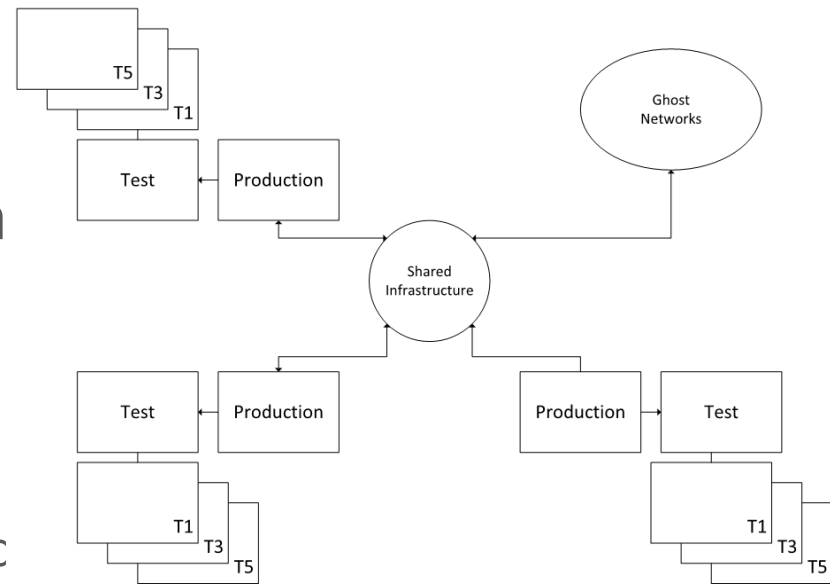
Here There Be Dragons



Started with Qualys for discovery and inventory
Installed Cloud Agent everywhere

Asset Grouping

- Asset Tags and Smart Tags were essential for making sense of the data
- Getting the right information to the right people
- Management teams flow into Business Units
 - which leads to environments, down to individual systems, and the teams who maintain them

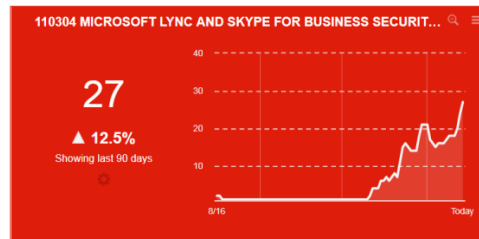


Reporting

Senior
Management

Team
Management

Operational
Staff



TOP 10 VULNERABILITIES	
VULNERABILITY TITLE	COUNT
Detected LanMan/NTLMv1 Authentication method	945
Intel Graphics Driver Multiple Vulnerabilities(INTEL-SA-00166)	800
Lenovo System Update Service Buffer Overflow Vulnerability	688
Windows Unquoted/Trusted Service Paths Privilege Escalation Securi...	670
Oracle Java SE Critical Patch Update - October 2018	516
VideoLAN VLC Media Player Arbitrary Code Execution Vulnerability	501
Infineon Trusted Platform Module (TPM) Chipsets Mishandles RSA k...	481

Senior Management Reporting

- Overall Risk instead of Vulnerability Reporting
- Trending – improving, stalled progress, trouble areas
- What BUs are the most risk? Do they need more attention?

Lessons Learned

Original assumptions changed after measuring with Qualys

Team Management Reporting

- Present Risks for their Area
 - Interval vs. Perimeter system
 - What is it running? What data does it have?
 - What systems and network does it connect to?
- Vulnerability Remediations vs. Trade-offs
- What is New? What is Fixed? What comes Back?
 - WLS-WSAT after October Patch



The Walking Dead

Operational Staff Reporting

- Prioritization based on Difficulty and Technical Details
 - Commercial software much easier to correct than open source
- Recommend Fixes: Patch, Configuration, Remove
- Where is the biggest bang for the buck?
 - Can one patch eliminate multiple issues?
 - How can Security shows this to IT?

Lessons Learned

1

Easy to get consumed by daily firefighting

“Work vs. Progress”

2

Management needs data and evidence to act

But don't confuse the issues with too much detail

3

Follow-up (without nagging)

Understand that operational teams have competing priorities

Q&A

Open Discussion

Michael Smith
TravelClick